REMARKS

The Office Action of September 15, 2009, has been received and reviewed. All pending claims stand rejected. Clarifying amendments are to be made to the application as previously set forth. All amendments and claim cancellations are made without prejudice or disclaimer. No new matter has been added. Reconsideration is respectfully requested.

35 U.S.C. § 102(b)

Claims 1-28 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent 6,327,578 to Linehan. The applicants respectfully traverse the rejection.

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Brothers v. Union Oil Co. of California*, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The identical invention must be shown in as complete detail as is contained in the claim. *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Furthermore, unless a single prior art reference describes "all of the limitations claimed" **and** "all of the limitations [are] **arranged or combined in the same way** as recited in the claim, it cannot be said to prove prior invention of the thing claimed and, thus, cannot anticipate under 35 U.S.C. § 102." *Net MoneyIN Inc. v. VeriSign Inc.*, 545 F.3d 1359, 1371 (Fed. Cir. 2008) (emphasis added). A single prior art reference must "clearly and unequivocally" describe the claimed invention "without *any* need for picking, choosing, and combining various disclosures not directly related to each other by the teachings of the cited reference." *Id.* (*citing In re Arkley*, 455 F.2d 586, 587 (C.C.P.A. 1972)).

Linehan attempts to improve the Secure Electronic Transaction ("SET") system. Linehan acknowledges SET as prior art (*see, e.g.*, col. 3, lines 6-10) and discusses SET at some length at column 3, as well as including a diagram of SET (FIG. 1) and noting the various differences between Linehan's system and SET (including how Linehan improves upon SET) at many points throughout the background information provided.

SET is a system for securing online transactions. While SET never succeeded in gaining great popularity, it was designed to function by giving the consumer a digital signature to use online instead of a credit card number, thus hiding the credit card number from the merchant.

The signature would be passed to the merchant, who would pass it to their acquiring bank, who would, in turn, pass it onto the issuing bank; the issuing bank would examine the signature and, if it was found to be valid and linked to an account with sufficient available credit, authorize the transaction and pass the authorization back to the acquiring bank, who would in turn pass it to the merchant.

After describing the SET system, Linehan states, at column 3, line 51 onwards:

> Where the wallet servers are run by issuing banks, it would be desirable to have the wallet servers directly authorize transactions before they are submitted to merchants. This would save the time and complexity required when the merchants obtain authorization from issuers through the merchant's acquiring banks. It would also be desirable to expand the cardholder authentication methods supported by the SET protocol, to enable an issuer to independently choose alternate authentication mechanisms without changing the acquirer gateway. As with any system, it would also be desirable to simplify the SET protocol in order to enable its easier implementation and to improve its overall performance.

Linehan then goes on to teach a "4 party protocol" wherein the consumer's PC is connected to both a merchant and the issuer's gateway and the merchant is then connected to the acquirer's gateway. According to Linehan, at column 7, line 14 onwards:

> In this manner, a "thin" wallet is enabled for the consumer in an electronic commerce protocol that is significantly simpler than the SET protocol, and that pre-authorizes payments thereby improving overall performance and enabling greater flexibility for issuer in the authentication of cardholders.

In Linehan, it appears that in most claimed embodiments, communication flow is as follows: it is initiated by the consumer's PC, which communicates with the merchant; the merchant replies to the consumer; the consumer communicates with the issuer gateway; the issuer gateway replies to the consumer; the consumer again communicates with the merchant and finally, the merchant communicates with the acquirer gateway.

Although Linehan states that "Many variations of this 4-party design are possible," the only variation detailed is one where, after the consumer communicates with the issuer gateway, the issuer gateway, rather than replying to the consumer, sends an authorization token to the merchant; the merchant then communicates confirmation to the consumer and subsequently submits the authorization token to the acquirer gateway. In all described network topologies,

therefore, Linehan requires direct communication between the consumer and the issuer gateway. Indeed, under "Discussion of the Preferred Embodiment" at column 5, lines 51-54, Linehan states "A principal feature of the invention is providing an issuer gateway and moving the credit/debit card authorization function from the merchant to the issuer thus enabling pre-authorization of payments."

Accordingly, Linehan does not change that basic system utilized by SET to attempt to provide security for on-line transactions. The principal feature which defines both SET and Linehan is the use of a digital certificate, linked to a particular user and account, which is stored in the form of a file on the consumer's computer and sent to third parties to verify the authenticity and payment capacity of the user.

One of the shortcomings of SET and similar systems -- and in applicants' view a principal reason why such schemes failed to gain popular acceptance -- is that they failed to provide EFTPOS equivalent security, authentication, or functionality. This is due to the above noted principal feature of SET and Linehan system, namely authentication of a user through the transmission of a digital certificate that is linked to a credit account held by a particular user and purports to authenticate that user and which is stored on a personal computer.

The difficulties with using such a method for authentication are multiple. First, the certificate is only as secure as the personal computer (which is notoriously insecure, particularly in the hands of less educated users). An attacker who is able to gain remote control of the computer could easily complete transactions from the user's computer and may well be able to obtain the certificate for future use from other computers.

Second, the certificate must be obtained through means such as applications, conducted outside of the described system, which may be insecure.

Third, the certificate is only linked to one particular account. If a user wishes to use other accounts they must obtain further certificates linked to those accounts through (possibly insecure) applications.

Fourth, such systems only enable the use of credit accounts, not debit accounts, for online transactions. This is because no facility exists for the entry or verification of a PIN, which is a prerequisite enforced by the banking industry for electronic debit transactions. Indeed, given the

lack of security of such systems, it is inconceivable that the banking industry would permit them to be used to store or transmit PINs.

It was as a reaction to such software based systems that the present applicants' Point of Pay or "PoP system" was designed. Rather than relying on a software component to try and make an insecure computer to computer transaction more secure, the philosophy behind PoP is to remove the processing and storage of any financial information from the computer altogether. The information is instead processed and transmitted by a separate, purpose made high security data entry device ("PoP Device") which creates its own secure connection to a banking network. The PoP Device has, in the preferred embodiment, a PIN pad and a card reader.

It is true that the PoP Device is, in the preferred embodiment, connected to a computer. However, for the purposes of the transmission of financial information, the computer is merely a "dumb terminal"; no financial or other personally identifying information is ever passed through the computer in an unencrypted form and any attacker would gain no advantage in terms of compromising the PoP system from gaining control of the computer (whether remotely or physically). The security provided by the PoP Device allows definitive authentication of the user and any information transmitted by the Device. This, in turn, allows the PoP system to be connected to the ATM network, as it provides security equivalent to an ATM or store front EFTPOS device.

A key aspect of the PoP claims, therefore, is a secure data entry device that is connected (via a network, such as the Internet) to a financial gateway which is in turn connected to the acquiring bank's financial switch (which forms part of the ATM network).

Aside from the required connections noted directly above, the network topology and communication flow of the PoP Claim, unlike the Linehan system, is highly flexible. While the PoP claim states "the gateway device includes means for transmitting the identifying information to the card-issuing financial institution", it is not necessary (nor envisioned) that the PoP gateway will be directly connected to the issuer's gateway or switch. Rather, the PoP gateway will connect to an acquirer's switch over a private network, which will in turn connect to the issuer's switch over another private network.

Linehan does mention a smart card reader at column 7, line 20. However, there are various substantial differences between a Linehan system with a smart card reader and a PoP system. First, the smart card reader is not a PIN entry device. Accordingly, the Linehan system in this configuration still lacks a means for securely entering and /or transmitting a PIN. Second, a smart card reader, dependent on its design, may not be able to definitively authenticate itself to a gateway. In such an arrangement, the primary authentication would continue to be performed using the digital certificate, including all its inherent flaws. Third, as a result of the lack of security, banking institutions would not permit such a system access to the ATM network and there would be no way to perform debit transactions.

The significant differences between Linehan and the present invention as defined in the amended claims and as discussed herein establish that Linehan does not anticipate the instant claims, and the rejections should be withdrawn.

The application is believed to be in condition for allowance, and an early notice thereof is respectfully solicited. Should the Examiner determine that additional issues remain which might be resolved by a telephone conference, the Examiner is respectfully invited to contact the applicants' undersigned attorney.

Respectfully submitted,

Allen C. Turner
Registration No. 33,041
Attorney for Applicants
TRASKBRITT, PC
P.O. Box 2550
Salt Lake City, Utah 84110-2550
Telephone: 801-532-1922

Date: March 11, 2010